WASHINGTON MILITARY DEPARTMENT POLICY

Administrative Policy 00-027-04 **INFORMATION TECHNOLOGY SECURITY**

This policy supercedes any Department policy issued on this subject with the same or similar title prior to the effective date of this policy.

1. PURPOSE: To establish the requirements for all employees on the protection and safeguard of computer assets and technology and agency-controlled data from destruction or compromise.

2. APPLICABILITY: This policy applies to all employees of the Washington Military Department (WMD), which includes state employees, federal employees, full-time, part-time, traditional guard members, and contractors who are or will be attached to the state governmental network through ".mil". Employees that are attached to the Army or Air National Guard networks must comply with the IT security policies that govern those networks. Commanders, managers, and supervisors are **not** authorized to make exceptions to this policy unless specifically authorized herein; however, they may impose tighter restrictions.

3. REFERENCES:

   a. Information Technology Security Policy, Adopted by the Information Services Board (ISB) on July 14, 2000 and amended April 2002.
   b. Information Technology Security Standards, Adopted by the Information Services Board (ISB) on November 20, 2000 and amended March 2003.
   c. Information Technology Security Guidelines, Adopted by the Information Services Board (ISB) on January 31, 2001 and amended June 2003.
   d. Information Technology Security Policy Audit Standards, Adopted by the State Auditor's Office on September 9, 2001.
   e. WMD Administrative Services Policy 00-004-04, Use of the Internet, Electronic Mail and Computer Systems, dated January 20, 2004.
   f. WMD Administrative Services Policy 07-00, Website Guidelines and Privacy Notice Information, dated March 2, 2001.
   g. WMD Administrative Services Policy 18-00, Telecommuting/Telework Policy, dated April 30, 2002.
   h. WMD Administrative Policy 05-00, Intellectual Property Protection, dated September 9, 2000.

4. POLICY: All users of WMD systems shall protect and use the Department's data and computer assets in an authorized manner. Failure to comply with this policy may result in corrective or disciplinary action up to and including termination of employment.

a. Roles and Responsibilities

(1) All WMD employees and authorized internal technology users must become familiar with information security policies, methods to protect agency data and proper use of WMD's electronic information and systems.

(2) Supervisors must ensure their employees are aware of and comply with Information Technology security policies for the proper use of computer resources and protecting Department data.

(3) Department divisions are responsible for the security of the information they collect, generate and/or manage.

(4) Non-WMD employees: All new external requests for computer access to electronic data and/or shared data must be submitted to the supervisor/manager or his/her designee in the area responsible for the data requested. Access will be granted or denied in accordance with pre-established procedures.

(5) The WMD Chief Information Officer (CIO) is responsible for the overall Information Technology Security Program.

(6) Information Technology Security Coordinators (ITSC) are considered agents of the CIO for Information Technology Security. ITSCs are appointed by members of the WMD Executive Management Team and will assist in implementing Information Technology security access policies and practices.

b. Electronic Security Awareness Training

(1) Initial IT Security Awareness Training:
WMD Human Resources staff will provide IT Security Awareness training as part of the Employee Orientation Checklist with each new employee.

(2) Annual Security Awareness Training:
All computer system users will complete annual security awareness training provided by the CIO or designated representatives.

c. Hardware Security Standards

(1) Only WMD or other Washington State Department owned or leased equipment may be connected to the WMD IT network.

(2) All technology (hardware, software, communications, etc.) purchased by, used at, or under the control of the WMD must meet applicable documented security standards. Where standards do not exist, the CIO will be consulted and security standards will be determined and applied.

(3) Users are responsible for maintaining physical control and security of portable devices including but not limited to: notebook computers, Tablet computers, Blackberry devices, Personal Digital Assistants (PDAs) and Cell Phones.

d. Software/Data Security

(1) Software use on Department IT equipment:

(a) Agency Standard software: The Department maintains standard suites of software, based upon unique mission authorizations, that have been tested and are compatible with the WMD Information Technology environment (see WMD Desktop Authorized Software List).

(b) All authorized WMD users will use the applicable standard software or authorized exception software for their respective division.

- (c) Exception software: Exception software is defined as software that is not found on the Department Standard Software List and is required to perform job duties. Exception software may be authorized only if there is a direct and substantial benefit to the employee's job performance and to the Department's business interests. Exception software purchase and use must be approved by the employee's Division Manager and by the CIO, and must comply with software licensing requirements.
- (d) Unauthorized software: Unauthorized software may not be used or loaded onto WMD network computers.
- (e) Security configurations: Workstations are configured to comply with the Department's and individual division's security and network standards. Users may not make unauthorized changes to configuration settings, including but not limited to security settings.
- (f) Software Testing: Network Managers will be authorized to install and test proposed new software packages and/or beta software products for the purpose of validating the software's compatibility with the Department's operating system software and other software packages.

(2) Electronic mail:

- (a) Employees will use only agency-authorized software for accessing Department e-mail.
- (b) Accessing private e-mail accounts for personal use is only authorized as specified in Administrative Services Policy 00-004-04.
- (c) Private e-mail accounts established for official business purposes must be approved in advance by the employee's supervisor and the respective division's IT Manager.

(3) Information stored on storage media:

- (a) Users are responsible for maintaining physical control and security of portable storage media (i.e. floppy disks, CD-ROMS, etc.)
- (b) Portable storage media that is used to contain sensitive data, such as sensitive inspection results or individuals' personal health information, must be secured.

(4) Disposing of storage media:

- (a) Internal computer storage media (hard drives, magnetic and optical storage media) must be cleaned in accordance with section 5, subsection 2 of Administrative Policy number 05-00, Intellectual Property Protection.
- (b) Magnetic and optical storage media (diskettes, tapes, etc.) must, likewise, be cleaned of data or destroyed.

(5) Reporting of violations, abuses, or misuses of WMD information and systems: WMD employees who become aware of suspected or potential violations or misuse of WMD information or systems should promptly report such information to their supervisor or military chain-of-command and to the CIO.

(6) Technical information:

Technical information such as network diagrams, internal network addresses or other sensitive technology information must be marked and presumed as "confidential" and will be made available only to authorized staff needing this information to perform their duties.

e. Access Security

(1) Categories of access:

(a) Computer logon accounts and passwords are the primary means of controlling access to the Department's electronically stored information. Access privileges must support adequate separation of duties to protect the Department's data.

(b) Supervisors are responsible for approving and submitting requests for categories of access granted to their staff. Most access requests are currently processed through the IT Security Coordinators, who process and track access requests. Access to systems and data is granted by the supervisor based on specific and current job duties.

(c) Any attempt to gain unauthorized access to information technology resources is strictly forbidden. Users must use only those information technology resources approved for their specific job responsibilities.

(d) Users must access or request confidential information only as required by their job duties.

(e) Users must access on-line computer systems using only a logon account for which they are authorized.

(f) Select support personnel (such as network administrators) have trusted access to ID and passwords for administrative support functions.

(2) Access changes:

(a) Supervisors must follow established procedures to notify system administrators of all system user terminations, transfers or changes before their effective date.

(b) Supervisors must follow procedures for any extended absences (over 30 days) so that logon accounts can be temporarily suspended.

(3) Emergency access:

The Department has the right to access, suspend or remove an employee's network, electronic mail or voice mail for operational investigative or disciplinary reasons.

(4) Screen saver for securing desktop:

All WMD computer users must lock and password protect their PCs when leaving their workstations. Timed screensaver activation must be set for 10 minutes or less. Alternate methods for securing the desktop are shutting down the PC or physically locking the office.

(5) Logon accounts:

Logon IDs must comply with WMD naming standards (see WMD Logon Id Naming Standard).

(6) Password security:

(a) Every computer user is responsible and accountable for all computer use under their logon account. The user logon account/password required for network access is equivalent to a legal signature.

(b) Users must access on-line computer systems using only a logon account for which they are authorized.

(c) An account password should not be disclosed to anyone except Information Technology support staff, if necessary, for computer maintenance. If a password has been disclosed, or is believed to be compromised, the user must change the password immediately. If your password has been compromised, immediately report it to your supervisor.

(d) Any temporary or new passwords given to a user will be changed by the user immediately.

(e) Hardened passwords are required for WMD applications and recommended for external (non-WMD) systems (see the WMD Password Management Standard).

(7) SCAN (State Controlled Area Network) authorization code security: SCAN authorization codes are used to prevent unauthorized use of the SCAN system. SCAN authorization codes should not be shared except where required to support the Emergency Management Division's Emergency Operations Center. If an authorization code is compromised, contact DCSIM Telecom Support to have the code changed.

(8) Remote access:

(a) Remote access for WMD staff - Authorized users must use established and Information Technology-approved secure access portals or services to access WMD's network from remote locations.

(b) Remote access for non-WMD staff – Will be permitted on a case-by-case basis with validation of the requirement by the appropriate member of the WMD Executive Management Team and approval of the CIO or his/her designee. Once authorized, users must use established and Information Technology-approved secure access portals or services to access WMD's network from remote locations.

(9) Wireless data access: Wireless data communication devices (e.g. notebooks, tablets, Personal Computers, cellular phones, PDAs, Blackberry devices, etc.) connecting to the WMD secure network, as a minimum, must meet Information Technology security standards as identified in Reference 3b..

(10) Dial-in telephone lines:

(a) Dial-in access is limited to instances where a more secure alternative is not available or is not cost justifiable. Requests for dial-in access through analog (modem) lines must be made to the unit's ITSC.

(b) The Information Technology Review Board (ITRB) will annually review the requirements for and use of dial-in lines.

5. This policy will be reviewed by the ITRB annually or more often, as deemed necessary. The ITRB will recommend changes and updates to the CIO who will review recommend changes with the WMD Executive Management Team and obtain approval of The Adjutant General.

The attached standards are hereby incorporated as part of this policy.

Timothy J. Lowenberg
Major General
The Adjutant General
Director, Washington Military Department

28 May 2004
Date

WMD DESKTOP AUTHORIZED SOFTWARE LIST
May 27, 2004

STANDARD DESKTOP SOFTWARE PACKAGE

1.	Operating System	-	Microsoft Windows 2000 or newer
2.	Office Suite	-	Microsoft Office Pro Office XP or newer
3.	PDF Reader	-	Adobe Acrobat Reader 5.0 or newer
4.	Anti Virus	-	McAfee Anti-Virus Version 7.0 or newer
5.	Internet Browser	-	Microsoft Internet Explorer 6.0 or newer
6.	Work Order Software	-	Track-It Web Client
7.	Instant Messenger	-	Microsoft Instant Messenger 4.7 or newer
8.	File Zipping Software	-	Winzip 8.1 or newer

SPECIALITY DESKTOP SOFTWARE APPLICATIONS
(Only installed on select Desktop Systems)

1.	VPN Client	-	Cisco VPN Client (where authorized)
2.	PDF Creation Software	-	Adobe Acrobat 5.0 or newer
3.	PDA Sync Software	-	Microsoft Active Sync 3.7 or newer
4.	Blackberry Software	-	Blackberry Desktop Manager 3.6
5.	CD Burning Software	-	Ahead Nero 5.10 or newer
6.	CD Burning Software	-	Roxio CD Creator 6.0 or newer
7.	TV Tuner Software	-	Hauppauge WINTV
8.	Java Software	-	Sun Java 2.4.1 or newer
9.	Mainframe Access Software	-	Attachmate EXTRA 95 or newer
10.	Diagramming software	-	Microsoft Visio 2000 or newer
11.	GIS/Mapping Software	-	Arcview 8.0 or newer
12.	GIS/Mapping Software	-	Mappoint
13.	Project Tracking Software	-	Microsoft Project 2000 or newer
14.	Electronic Filing Software	-	Ecopy Software
15.	DVD Playing Software	-	PowerDVD
16.	Reporting Software	-	Crystal Reports Version 9.0 or newer
17.	Drawing Software	-	Smart Draw
18.	Plume Modeling Software	-	D2Puff Client 4.2 or newer
19.	Telnet terminal emulator	-	TeraTerm Pro
20.	Telnet terminal emulator	-	ProComm Pro
21.	DVD Playing Software	-	InterVideo
22.	Screen Capture Software	-	Keyprint
23.	Screen Capture Software	-	Hoversnap
24.	SSH Terminal emulator	-	Putty
25.	Password Auditing Software	-	LC4
26.	DVD Creation Software	-	Sonic My DVD
27.	KVM Administrative Software	-	Black Box KVM

28.	Drawing Software	-	AutoCad LT v2004
29.	Microwave Monitoring Software	-	Smart Scan
30.	File and folder encryption	-	Mooseoft Encryption
31.	FTP Software	-	WS FTP
32.	E-file shredder program	-	Eraser 5.1
33.	Multi media player	-	Windows Media Player 8.0 or newer
34.	Multi media player	-	Quick Time Player 6.5 or newer
35.	Multi media player	-	Real Player 10.0 or newer\
36.	Emergency Alert Software	-	ENDEC PRO
37.	Emergency Satellite System	-	EMnet and EAS Watch
38.	Drawing	-	MSFT Visio
39.	Drawing file viewer	-	Volo View Express
40.	Internet information mgt	-	Macromedia Contribute
41.	CSEPP Mgt software	-	CSEPP CA Tools
42.	USCG Mapping tools	-	Corpswin.exe
43.	Radio Engr Software	-	PathLoss 4.0
44.	Radio Freq Mgt Software	-	Slattery Software v2.57A
45.	Radio Freq database	-	Percon

WMD LOGON ID NAMING STANDARD
May 27, 2004

WMD Logon IDs are created using the requirements and guidelines established by the Washington State Enterprise Active Directory Forest in the "Naming Conventions and Standards Document", version 3.0, dated 15 June 2001 and located at URL: http://sww.wa.gov/win2k/approved/docs/WALCL%20Naming%20Conventions%20and%20Standards%203.0.doc .

The standard WMD Logon ID name is: **xxx245** where xxx is the user's first, middle, and last initial and 245 is the Department's agency number. In the event of duplicate first, middle and last initials, the Logon ID will be the first two letters of the first name followed by the last initial followed by 245.

Authorized exceptions to this policy only apply to the WEBEOC and D2Puff applications, at this time, due to the access to these programs by outside agencies via individual clients.

WMD PASSWORD MANAGEMENT STANDARD
May 27, 2004

System (network) passwords have the following characteristics:

- Passwords must be a minimum of 8 characters long and contain at least one special character and 2 of the following 3 character classes: upper case letters, lower case letters, and numerals
- Must not contain employee's user name or any part of their full name
- Passwords must be changed a minimum of every 90 days, but not before 78 days
- Password administration rules are systematically enforced; users are prompted in advance for normal cyclic password changes
- For compromised or lost passwords, user notifies administrator who immediately changes password. To preserve password privacy, on first logon by user with assigned password, user is prompted by system for a new password.

Department applications such as WebEOC, Contract Management System and Electronic Purchase Order have separate password administration by designated program staff.